UNITED STATES DISTRICT COURT
DISTRICT OF MARYLAND

In re Lafayette Federal Credit Union Data Breach Litigation	Master File No. 8:25-cv-01006-DLB
This Document Relates To: All Actions	**JURY TRIAL DEMANDED**

CONSOLIDATED CLASS ACTION COMPLAINT

COMES NOW Ricardo Aviles, Kristine Darbinyan, Sebhia Dibra, Carl Lewis, Joseph Mausteller, Paul Richards, and Andy Wang ("Plaintiffs"), individually and behalf of all citizens who are similarly situated, for their Consolidated Class Action Complaint against Lafayette Federal Credit Union ("Defendant" or "LFCU") and allege, upon personal knowledge as to their own actions and their counsels' investigation, and upon information and belief as to all other matters, as follows:

I. INTRODUCTION

1. Plaintiffs bring this class action against Defendant for their failure to exercise reasonable care in securing and safeguarding individuals' sensitive personal data.

2. In order to provide financial services to Plaintiffs and Class members, Defendant required Plaintiffs and Class members to provide their Private Information to Defendant.

3. On September 16, 2024, Defendant LFCU experienced a data breach incident ("Data Breach"). The types of personal data exposed included names, financial account information, loan account numbers, and Social Security numbers (collectively "Private Information" or "PII").

4. On or about March 20, 2025, Plaintiffs received a Notice of Data Breach letter (the "Notice Letter") describing the breach of their Private Information.

5. Defendant's security failures enabled the hackers to steal the Private Information of Plaintiffs and members of the Class (defined below). These failures put Plaintiffs' and Class members' Private Information and interests at serious, immediate, and ongoing risk. As a result of the Data Breach, Plaintiffs and Class members suffered concrete injuries in fact including, but not limited to: (i) lost time, productivity, and opportunity costs associated with attempting to mitigate the actual and future consequences of the Data Breach including, as appropriate, reviewing records for fraudulent charges, reissuing payment cards, purchasing credit monitoring and identity theft protection services, imposition of withdrawal and purchase limits on compromised accounts, and initiating and monitoring credit freezes; (ii) invasion of their privacy; (iii) theft of their PII; (iv) lost or diminished value of their PII; (v) loss of benefit of the bargain; (vi) nominal damages; (vii) the continued and certainly increased risk to cybercriminals accessing their PII, which (a) remains unencrypted and available for unauthorized third parties to access and abuse, and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII; and (viii) suffering from fear, anxiety, and stress associated with constantly having to monitor personal banking and credit accounts due to their PII now being in the hands of cybercriminals.

6. The Data Breach was caused and enabled by Defendant's violation of their obligations to abide by best practices and industry standards concerning the security of consumers' records and Private Information. Defendant failed to comply with security standards and allowed their customers' Private Information to be compromised by cutting corners on security measures that could have prevented or mitigated the Data Breach that occurred.

7. Accordingly, Plaintiffs and Class members assert claims for negligence, breach of implied contract, unjust enrichment, negligence *per se*, breach of fiduciary duty, and invasion of

privacy, and seek injunctive relief, monetary damages, and all other relief as authorized in equity or by law. Plaintiffs Darbinyan and Lewis and California Subclass members additionally assert claims for violation of the California Unfair Competition Law and violation of the California Consumer Privacy Act.

II. JURISDICTION AND VENUE

8. This Court has original jurisdiction over this action under the Class Action Fairness Act, 28 U.S.C. § 1332(d)(2), because (i) at least one member of the putative Class, as defined below, is a citizen of a different state than Defendant, (ii) there are more than 100 putative Class members, and (iii) the amount in controversy exceeds $5 million, exclusive of interest and costs.

9. This Court has general personal jurisdiction over Defendant because Defendant maintains its principal place of business in this District, regularly conducts business in Maryland, and has sufficient minimum contacts in Maryland.

10. Venue is proper in this Court pursuant to 28 U.S.C. § 1391(b) because Defendant maintains its principal place of business in this District and therefore resides in this District pursuant to 28 U.S.C. § 1391(c)(2). A substantial part of the events, acts, and omissions giving rise to Plaintiffs' and the Class's claims also occurred in this District.

III. PARTIES

A. Plaintiffs

1. Plaintiff Ricardo Aviles

11. Plaintiff Aviles is a resident and citizen of Florida.

12. Plaintiff Aviles is a current customer of LFCU.

13. Plaintiff Aviles provided his Private Information to Defendant as a condition for receiving banking and financial services. He provided this information on the condition that it be

maintained as confidential and with the understanding that Defendant would employ reasonable safeguards to protect his Private Information. If Plaintiff Aviles had known that Defendant would not adequately protect his Private Information, he would not have entrusted Defendant with his Private Information or allowed Defendant to maintain this sensitive Private Information.

14. In order to obtain financial services from Defendant, Plaintiff Aviles was required to provide his Private Information to Defendant.

15. Upon information and belief, Plaintiff Aviles's Private Information was within the possession and control of Defendant at the time of the Data Breach.

16. Plaintiff Aviles is very careful about sharing his Private Information. Plaintiff Aviles stores any documents containing his Private Information in a safe and secure location or destroys the documents. He has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

17. Plaintiff Aviles became aware of the Data Breach through a Notice Letter dated March 20, 2025.

18. As a result of the Data Breach, Plaintiff Aviles made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching and verifying the legitimacy of the Data Breach as well as self-monitoring his financial accounts and credit reports for any indication of fraudulent activity, which may take years to detect. Plaintiff Aviles has spent significant time remedying the breach—valuable time Plaintiff Aviles otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

19. Even with the best response, the harm caused to Plaintiff Aviles cannot be undone.

20. Plaintiff Aviles suffered actual injury from having his Personal Information compromised as a result of the Data Breach including, but not limited to: (i) the theft of his PII; (ii) diminution of value of his PII; (iii) invasion of privacy; (iv) loss of benefit of the bargain; (v) lost time spent on activities remedying harms resulting from the Data Breach; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) annoyance, interference, and inconvenience as a result of attempting to mitigate the actual consequences of the Data Breach; and (viii) the continued and increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

21. Plaintiff Aviles has suffered an increase in spam calls and text messages since the Data Breach.

22. The Data Breach has caused Plaintiff Aviles to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant did not immediately notify him of the incident and the fact that Defendant still has not fully informed him of key details about the Data Breach and the information stolen.

23. As a result of the Data Breach, Plaintiff Aviles anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harm caused by the Data Breach. As a result of the Data Breach, Plaintiff Aviles is at present risk and will continue to be at increased risk of identity theft and fraud for years to come.

24. The risk of identity theft is impending and has materialized, as there is evidence that Plaintiff Aviles's and Class members' PII was targeted, accessed, and misused, including through likely publication and dissemination on the dark web. Plaintiff Aviles further believes his

PII, and that of Class members, was and will be sold and disseminated on the dark web following the Data Breach as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

25. Plaintiff Aviles has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

2. Plaintiff Kristine Darbinyan

26. Plaintiff Darbinyan is a resident and citizen of the State of California.

27. Plaintiff Darbinyan is a current customer of LFCU.

28. Plaintiff Darbinyan provided her Private Information to Defendant as a condition for receiving banking and financial services. She provided this information on the condition that it be maintained as confidential and with the understanding that Defendant would employ reasonable safeguards to protect her Private Information. If Plaintiff Darbinyan had known that Defendant would not adequately protect her Private Information, she would not have entrusted Defendant with her Private Information or allowed Defendant to maintain this sensitive Private Information.

29. Plaintiff Darbinyan has been using Defendant's services since 2023.

30. In order to obtain financial services from Defendant, Plaintiff Darbinyan was required to provide her Private Information to Defendant.

31. Upon information and belief, Plaintiff Darbinyan's Private Information was within the possession and control of Defendant at the time of the Data Breach.

32. Plaintiff Darbinyan is very careful about sharing her Private Information. Plaintiff Darbinyan stores any documents containing her Private Information in a safe and secure location

or destroys them. She has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

33. At the time of the Data Breach, Defendant retained Plaintiff Darbinyan's PII in its network systems with inadequate data security, causing Plaintiff Darbinyan's PII to be accessed and exfiltrated by cybercriminals in the Data Breach.

34. Plaintiff Darbinyan became aware of the Data Breach through a Notice Letter dated March 20, 2025. The Notice Letter informed Plaintiff Darbinyan that her PII was accessed and exposed to unauthorized hackers in the Data Breach. According to the Notice Letter, the hackers acquired files containing Plaintiff Darbinyan's sensitive PII, including her name, Social Security number, and financial account number.

35. As a result of the Data Breach, Plaintiff Darbinyan made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching and verifying the legitimacy of the Data Breach as well as self-monitoring her financial accounts and credit reports for any indication of fraudulent activity, which may take years to detect. Plaintiff Darbinyan continues to monitor her financial and credit statements multiple times a week. Plaintiff has spent significant time remedying the breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

36. Even with the best response, the harm caused to Plaintiff Darbinyan cannot be undone.

37. Plaintiff Darbinyan suffered actual injury from having her Personal Information compromised as a result of the Data Breach including, but not limited to: (i) the theft of her PII;

(ii) diminution of value of her PII; (iii) invasion of privacy; (iv) loss of benefit of the bargain; (v) lost time spent on activities remedying harms resulting from the Data Breach; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) annoyance, interference, and inconvenience as a result of attempting to mitigate the actual consequences of the Data Breach; and (viii) the continued and increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

38. Plaintiff Darbinyan has suffered an increase in spam calls and text messages since the Data Breach.

39. The Data Breach has caused Plaintiff Darbinyan to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant did not immediately notify her of the incident and the fact that Defendant still has not fully informed her of key details about the Data Breach and the information stolen.

40. As a result of the Data Breach, Plaintiff Darbinyan anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harm caused by the Data Breach. As a result of the Data Breach, Plaintiff Darbinyan is at present risk and will continue to be at increased risk of identity theft and fraud for years to come.

41. The risk of identity theft is impending and has materialized, as there is evidence that Plaintiff Darbinyan's and Class members' PII was targeted, accessed, and misused, including through likely publication and dissemination on the dark web. Plaintiff Darbinyan further believes her PII, and that of Class members, was and will be sold and disseminated on the dark web

following the Data Breach as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

42. Plaintiff Darbinyan has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

3. Plaintiff Sebhia Dibra

43. Plaintiff Dibra is a resident and citizen of New York.

44. Plaintiff Dibra is a former customer of LFCU.

45. Plaintiff Dibra provided her Private Information to Defendant as a condition for receiving banking and financial services. She provided this information on the condition that it be maintained as confidential and with the understanding that Defendant would employ reasonable safeguards to protect her Private Information. If Plaintiff Dibra had known that Defendant would not adequately protect her Private Information, she would not have entrusted Defendant with her Private Information or allowed Defendant to maintain this sensitive Private Information.

46. In order to obtain financial services from Defendant, Plaintiff Dibra was required to provide her Private Information to Defendant.

47. Upon information and belief, Plaintiff Dibra's Private Information was within the possession and control of Defendant at the time of the Data Breach.

48. Plaintiff Dibra is very careful about sharing her Private Information. Plaintiff Dibra stores any documents containing her Private Information in a safe and secure location or destroys the documents. She has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source. Moreover, she diligently chooses unique usernames and passwords for her various online accounts.

49. At the time of the Data Breach, Defendant retained Plaintiff Dibra's PII in its network systems with inadequate data security, causing Plaintiff Dibra's PII to be accessed and exfiltrated by cybercriminals in the Data Breach.

50. Plaintiff Dibra became aware of the Data Breach through a Notice Letter dated March 20, 2025. The Notice Letter informed Plaintiff Dibra that her PII was accessed and exposed to unauthorized hackers in the Data Breach. According to the Notice Letter, the hackers acquired files containing Plaintiff Dibra's sensitive PII, including her name, Social Security number, financial account number, and loan account number.

51. As a result of the Data Breach, Plaintiff Dibra made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching and verifying the legitimacy of the Data Breach as well as self-monitoring her financial accounts and credit reports for any indication of fraudulent activity, which may take years to detect. Plaintiff Dibra continues to monitor her financial and credit statements multiple times a week. Plaintiff has spent significant time remedying the breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

52. Even with the best response, the harm caused to Plaintiff Dibra cannot be undone.

53. Plaintiff Dibra suffered actual injury from having her Personal Information compromised as a result of the Data Breach including, but not limited to: (i) the theft of her PII; (ii) diminution of value of her PII; (iii) invasion of privacy; (iv) loss of benefit of the bargain; (v) lost time spent on activities remedying harms resulting from the Data Breach; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) annoyance, interference, and inconvenience as a result of attempting to mitigate the actual

consequences of the Data Breach; and (viii) the continued and increased risk to her PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

54. Plaintiff Dibra has suffered an increase in spam calls and text messages since the Data Breach.

55. The Data Breach has caused Plaintiff Dibra to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant did not immediately notify her of the incident and the fact that Defendant still has not fully informed her of key details about the Data Breach and the information stolen.

56. As a result of the Data Breach, Plaintiff Dibra anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harm caused by the Data Breach. As a result of the Data Breach, Plaintiff Dibra is at present risk and will continue to be at increased risk of identity theft and fraud for years to come.

57. The risk of identity theft is impending and has materialized, as there is evidence that Plaintiff Dibra's and Class members' PII was targeted, accessed, and misused, including through likely publication and dissemination on the dark web. Plaintiff Dibra further believes her PII, and that of Class members, was and will be sold and disseminated on the dark web following the Data Breach as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

58. Plaintiff Dibra has a continuing interest in ensuring that her Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

4. Plaintiff Carl Lewis

59. Plaintiff Lewis is a resident and citizen of California.

60. Plaintiff Lewis is a former customer of LFCU.

61. Plaintiff Lewis provided his Private Information to Defendant as a condition for receiving banking and financial services. He provided this information on the condition that it be maintained as confidential and with the understanding that Defendant would employ reasonable safeguards to protect his Private Information. If Plaintiff Lewis had known that Defendant would not adequately protect his Private Information, he would not have entrusted Defendant with his Private Information or allowed Defendant to maintain this sensitive Private Information.

62. Plaintiff Lewis used Defendant's services from 2001 until 2006.

63. In order to obtain financial services from Defendant, Plaintiff Lewis was required to provide his Private Information to Defendant.

64. Upon information and belief, Plaintiff Lewis's Private Information was within the possession and control of Defendant at the time of the Data Breach.

65. Plaintiff Lewis is very careful about sharing his Private Information. Plaintiff Lewis stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

66. At the time of the Data Breach, Defendant retained Plaintiff Lewis's PII in its network systems with inadequate data security, causing Plaintiff Lewis's PII to be accessed and exfiltrated by cybercriminals in the Data Breach.

67. Plaintiff Lewis became aware of the Data Breach through a Notice Letter dated March 20, 2025. The Notice Letter informed Plaintiff Lewis that his PII was accessed and exposed to unauthorized hackers in the Data Breach. According to the Notice Letter, the hackers acquired files containing Plaintiff Lewis's sensitive PII, including his name, date of birth, Social Security number, and financial account number.

68. As a result of the Data Breach, Plaintiff Lewis made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching and verifying the legitimacy of the Data Breach as well as self-monitoring his financial accounts and credit reports for any indication of fraudulent activity, which may take years to detect. Plaintiff Lewis continues to monitor his financial and credit statements multiple times a week. Plaintiff has spent significant time remedying the breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

69. Even with the best response, the harm caused to Plaintiff Lewis cannot be undone.

70. Plaintiff Lewis suffered actual injury from having his Personal Information compromised as a result of the Data Breach including, but not limited to: (i) the theft of his PII; (ii) diminution of value of his PII; (iii) invasion of privacy; (iv) loss of benefit of the bargain; (v) lost time spent on activities remedying harms resulting from the Data Breach; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) annoyance, interference, and inconvenience as a result of attempting to mitigate the actual consequences of the Data Breach; and (viii) the continued and increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b)

remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

71. Plaintiff Lewis has suffered an increase in spam calls and text messages since the Data Breach.

72. Plaintiff Lewis has also suffered actual damages in that he has been notified on a password application that he purchased, that seven of his accounts have compromised passwords. Upon information and belief this is a result of the Data Breach.

73. The Data Breach has caused Plaintiff Lewis to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant did not immediately notify him of the incident and the fact that Defendant still has not fully informed him of key details about the Data Breach and the information stolen.

74. As a result of the Data Breach, Plaintiff Lewis anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harm caused by the Data Breach. As a result of the Data Breach, Plaintiff Lewis is at present risk and will continue to be at increased risk of identity theft and fraud for years to come.

75. The risk of identity theft is impending and has materialized, as there is evidence that Plaintiff Lewis's and Class members' PII was targeted, accessed, and misused, including through likely publication and dissemination on the dark web. Plaintiff Lewis further believes his PII, and that of Class members, was and will be sold and disseminated on the dark web following the Data Breach as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

76. Plaintiff Lewis has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

5. Plaintiff Joseph Mausteller

77. Plaintiff Mausteller has resided in North Carolina for the time period relevant to this Data Breach.

78. Plaintiff Mausteller is a current customer of LFCU.

79. Plaintiff Mausteller provided his Private Information to Defendant as a condition for receiving banking and financial services. He provided this information on the condition that it be maintained as confidential and with the understanding that Defendant would employ reasonable safeguards to protect his Private Information. If Plaintiff Mausteller had known that Defendant would not adequately protect his Private Information, he would not have entrusted Defendant with his Private Information or allowed Defendant to maintain this sensitive Private Information.

80. Plaintiff Mausteller has been using Defendant's services since October 2020.

81. In order to obtain financial services from Defendant, Plaintiff Mausteller was required to provide his Private Information to Defendant.

82. Upon information and belief, Plaintiff Mausteller's Private Information was within the possession and control of Defendant at the time of the Data Breach.

83. Plaintiff Mausteller is very careful about sharing his Private Information. Plaintiff Mausteller stores any documents containing his Private Information in a safe and secure location. He has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

84. At the time of the Data Breach, Defendant retained Plaintiff Mausteller's PII in its network systems with inadequate data security, causing Plaintiff Mausteller's PII to be accessed and exfiltrated by cybercriminals in the Data Breach.

85. Plaintiff Mausteller became aware of the Data Breach through a Notice Letter dated March 20, 2025. The Notice Letter informed Plaintiff Mausteller that his PII was accessed and exposed to unauthorized hackers in the Data Breach. According to the Notice Letter, the hackers acquired files containing Plaintiff Mausteller's sensitive PII, including his name, loan account number, Social Security number, and financial account number.

86. As a result of the Data Breach, Plaintiff Mausteller made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching and verifying the legitimacy of the Data Breach as well as self-monitoring his financial accounts and credit reports for any indication of fraudulent activity, which may take years to detect. Plaintiff Mausteller continues to monitor his financial and credit statements multiple times a week. Plaintiff has spent significant time remedying the breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

87. Even with the best response, the harm caused to Plaintiff Mausteller cannot be undone.

88. Plaintiff Mausteller suffered actual injury from having his Personal Information compromised as a result of the Data Breach including, but not limited to: (i) the theft of his PII; (ii) diminution of value of his PII; (iii) invasion of privacy; (iv) loss of benefit of the bargain; (v) lost time spent on activities remedying harms resulting from the Data Breach; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii)

annoyance, interference, and inconvenience as a result of attempting to mitigate the actual consequences of the Data Breach; and (viii) the continued and increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

89. On or around March 4, 2025, Plaintiff Mausteller received a Lafayette Fraud Alert notifying him of an unauthorized transaction related to Google on his LFCU debit card. Subsequently, Plaintiff Mausteller had his debit card replaced.

90. Plaintiff Mausteller has suffered an increase in spam calls and text messages since the Data Breach.

91. The Data Breach has caused Plaintiff Mausteller to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant did not immediately notify him of the incident and the fact that Defendant still has not fully informed him of key details about the Data Breach and the information stolen.

92. As a result of the Data Breach, Plaintiff Mausteller anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harm caused by the Data Breach. As a result of the Data Breach, Plaintiff Mausteller is at present risk and will continue to be at increased risk of identity theft and fraud for years to come.

93. The risk of identity theft is impending and has materialized, as there is evidence that Plaintiff Mausteller's and Class members' PII was targeted, accessed, and misused, including through likely publication and dissemination on the dark web. Plaintiff Mausteller further believes his PII, and that of Class members, was and will be sold and disseminated on the dark web

following the Data Breach as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

94. Plaintiff Mausteller has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

6. Plaintiff Paul Richards

95. Plaintiff Richards is a resident and citizen of Greenbelt, Maryland.

96. Plaintiff Richards is a current customer of LFCU.

97. Plaintiff Richards provided his Private Information to Defendant as a condition of receiving banking and financial services. He provided this information on the condition that it be maintained as confidential and with the understanding that Defendant would employ reasonable safeguards to protect his Private Information. If Plaintiff Richards had known that Defendant would not adequately protect his Private Information, he would not have entrusted Defendant with his Private Information or allowed Defendant to maintain this sensitive Private Information.

98. In order to obtain financial services from Defendant, Plaintiff Richards was required to provide his Private Information to Defendant.

99. Upon information and belief, Plaintiff Richards's Private Information was within the possession and control of Defendant at the time of the Data Breach.

100. Plaintiff Richards is very careful about sharing his Private Information. Plaintiff Richards stores any documents containing his Private Information in a safe and secure location or destroys them. He has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

101. At the time of the Data Breach, Defendant retained Plaintiff Richards's PII in its network systems with inadequate data security, causing Plaintiff Richards's PII to be accessed and exfiltrated by cybercriminals in the Data Breach.

102. Plaintiff Richards became aware of the Data Breach through a Notice Letter dated March 20, 2025. The Notice Letter informed Plaintiff Richards that his PII was accessed and exposed to unauthorized hackers in the Data Breach. According to the Notice Letter, the hackers acquired files containing Plaintiff Richards's sensitive PII, including his name, Social Security number, and financial account number.

103. As a result of the Data Breach, Plaintiff Richards made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to researching and verifying the legitimacy of the Data Breach as well as self-monitoring his financial accounts and credit reports for any indication of fraudulent activity, which may take years to detect. Plaintiff Richards continues to monitor his financial and credit statements multiple times a week. Plaintiff has spent significant time remedying the breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

104. Even with the best response, the harm caused to Plaintiff Richards cannot be undone.

105. Plaintiff Richards suffered actual injury from having his Personal Information compromised as a result of the Data Breach including, but not limited to: (i) the theft of his PII; (ii) diminution of value of his PII; (iii) invasion of privacy; (iv) loss of benefit of the bargain; (v) lost time spent on activities remedying harms resulting from the Data Breach; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii)

annoyance, interference, and inconvenience as a result of attempting to mitigate the actual consequences of the Data Breach; and (viii) the continued and increased risk to his PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

106. Plaintiff Richards has suffered an increase in spam calls and text messages since the Data Breach.

107. The Data Breach has caused Plaintiff Richards to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant did not immediately notify him of the incident and the fact that Defendant still has not fully informed him of key details about the Data Breach and the information stolen.

108. As a result of the Data Breach, Plaintiff Richards anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harm caused by the Data Breach. As a result of the Data Breach, Plaintiff Richards is at present risk and will continue to be at increased risk of identity theft and fraud for years to come.

109. The risk of identity theft is impending and has materialized, as there is evidence that Plaintiff Richards's and Class members' PII was targeted, accessed, and misused, including through likely publication and dissemination on the dark web. Plaintiff Richards further believes his PII, and that of Class members, was and will be sold and disseminated on the dark web following the Data Breach as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

110. Plaintiff Richards has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

7. Plaintiff Andy Wang

111. Plaintiff Wang is a resident and citizen of the District of Columbia.

112. Plaintiff Wang is a current customer of LFCU.

113. Plaintiff Wang provided his Private Information to Defendant as a condition for receiving banking and financial services. He provided this information on the condition that it be maintained as confidential and with the understanding that Defendant would employ reasonable safeguards to protect his Private Information. If Plaintiff Wang had known that Defendant would not adequately protect his Private Information, he would not have entrusted Defendant with his Private Information or allowed Defendant to maintain this sensitive Private Information.

114. Plaintiff Wang has been using Defendant's services since 2024.

115. In order to obtain financial services from Defendant, Plaintiff Wang was required to provide his Private Information to Defendant.

116. Upon information and belief, Plaintiff Wang's Private Information was within the possession and control of Defendant at the time of the Data Breach.

117. Plaintiff Wang is very careful about sharing his Private Information. Plaintiff Wang stores any documents containing his Private Information in a safe and secure location or destroys them. He has never knowingly transmitted unencrypted sensitive Private Information over the Internet or any other unsecured source. Moreover, he diligently chooses unique usernames and passwords for his various online accounts.

118. At the time of the Data Breach, Defendant retained Plaintiff Wang's PII in its network systems with inadequate data security, causing Plaintiff Wang's PII to be accessed and exfiltrated by cybercriminals in the Data Breach.

119. Plaintiff Wang became aware of the Data Breach through a Notice Letter dated March 20, 2025. The Notice Letter informed Plaintiff Wang that his PII was accessed and exposed to unauthorized hackers in the Data Breach. According to the Notice Letter, the hackers acquired files containing Plaintiff Wang's sensitive PII, including his name and financial account number.

120. As a result of the Data Breach, Plaintiff Wang made reasonable efforts to mitigate the impact of the Data Breach, including but not limited to: researching and verifying the legitimacy of the Data Breach as well as self-monitoring his financial accounts, medical records, and credit reports for any indication of fraudulent activity, which may take years to detect. Plaintiff Wang continues to monitor his financial and credit statements multiple times a week. Plaintiff Wang has spent significant time remedying the breach—valuable time Plaintiff otherwise would have spent on other activities, including but not limited to work and/or recreation. This time has been lost forever and cannot be recaptured.

121. Even with the best response, the harm caused to Plaintiff Wang cannot be undone.

122. Plaintiff Wang suffered actual injury from having his Personal Information compromised as a result of the Data Breach including, but not limited to: : (i) the theft of his PII; (ii) diminution of value of his PII; (iii) invasion of privacy; (iv) loss of benefit of the bargain; (v) lost time spent on activities remedying harms resulting from the Data Breach; (vi) lost opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (vii) annoyance, interference, and inconvenience as a result of attempting to mitigate the actual consequences of the Data Breach; (viii) the continued and increased risk to his PII, which: (a)

remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

123. Plaintiff Wang has suffered an increase in spam calls and text messages since the Data Breach.

124. The Data Breach has caused Plaintiff Wang to suffer fear, anxiety, and stress, which has been compounded by the fact that Defendant did not immediately notify him of the incident and the fact that Defendant still has not fully informed him of key details about the Data Breach and the information stolen.

125. As a result of the Data Breach, Plaintiff Wang anticipates spending considerable time and money on an ongoing basis to try to mitigate and address harm caused by the Data Breach. As a result of the Data Breach, Plaintiff Wang is at present risk and will continue to be at increased risk of identity theft and fraud for years to come.

126. The risk of identity theft is impending and has materialized, as there is evidence that Plaintiff Wang's and Class members' PII was targeted, accessed, and misused, including through likely publication and dissemination on the dark web. Plaintiff Richards further believes his PII, and that of Class members, was and will be sold and disseminated on the dark web following the Data Breach as that is the *modus operandi* of cybercriminals that commit cyber-attacks of this type.

127. Plaintiff Wang has a continuing interest in ensuring that his Private Information, which, upon information and belief, remains backed up in Defendant's possession, is protected and safeguarded from future breaches.

B. Defendant Lafayette Federal Credit Union

128. Defendant Lafayette Federal Credit Union is a company with its principal place of business located in Rockville, Maryland.[1]

129. Defendant LFCU's privacy policy states that it will protect members' privacy and will "use security measures that comply with federal law. These measures include computer safeguards and secured files and buildings. We maintain physical, electronic, and procedural safeguards that comply with federal regulations to guard your non-public personal information."[2]

IV. BACKGROUND FACTS

A. Defendant's Business

130. Defendant LFCU is a financial institution that operates eight full-service branch locations in Virginia, Maryland, and the District of Columbia.

131. Over the course of their relationship, customers, including Plaintiffs and Class members, provided Defendant with their sensitive PII.

B. The Data Breach

132. On or about March 20, 2025, Defendant began sending Plaintiffs and other Data Breach victims a Notice of Data Breach letter (the "Notice Letter"), stating:

> **What Happened?** We recently learned that an unknown, unauthorized third party gained access to one LFCU employee email account. Upon discovering the incident, we promptly secured the email account and began an internal investigation. We also engaged a forensic security firm to investigate and confirm the security of our email systems. The investigation determined that an unauthorized third party accessed the email account for a brief period on September 16, 2024, and may have acquired the information contained in the account.[3]

[1] LAFAYETTE FEDERAL CREDIT UNION, https://www.lfcu.org/contact/ (last accessed May 27, 2025).
[2] LAFAYETTE FEDERAL CREDIT UNION, https://www.lfcu.org/privacy-policy/ (last accessed May 27, 2025).
[3] See Exs. 1-2, Plaintiff's Dibra and Wang's notice letters.

133. Defendant has yet to affirmatively notify impacted parties individually regarding which specific pieces of their Private Information were stolen.

134. The Data Breach occurred because Defendant failed to take reasonable measures to protect the Private Information they collected and stored. Among other things, Defendant failed to implement data security measures designed to prevent this attack, despite repeated public warnings to the financial industry about the risk of cyberattacks and the highly publicized occurrence of many similar attacks in the recent past on financial institutions. For example, Defendant failed to maintain basic security measures. Defendant failed to disclose to Plaintiff and Class members the material fact that it did not have adequate data security practices to safeguard customers' personal data, and in fact falsely represented that their security measures were sufficient to protect the Personal Information in their possession.

135. Defendant's failure to provide immediate formal notice of the Breach to Plaintiffs and Class members exacerbated the injuries resulting from the Breach.

C. Defendant Failed to Maintain Reasonable and Adequate Security Measures to Safeguard Consumers' Private Information Despite Previous Data Breaches

136. Defendant was or should have been aware of the risk of data breaches, especially as data breaches in the banking industry are becoming exponentially more common.

137. As explained by the Federal Bureau of Investigation, "[p]revention is the most effective defense against ransomware and it is critical to take precautions for protection."[4]

138. To prevent and detect cyberattacks and/or ransomware attacks, Defendant could and should have implemented, as recommended by the United States Government, the following measures:

[4] Federal Bureau of Investigation, *How to Protect Your Networks from Ransomware*, https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view.

- Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

- Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

- Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

- Configure firewalls to block access to known malicious IP addresses.

- Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

- Set anti-virus and anti-malware programs to conduct regular scans automatically.

- Consider disabling Remote Desktop protocol (RDP) if it is not being used.

- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.

- Execute operating system environments or specific programs in a virtualized environment.

- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.[5]

139. The occurrence of the Data Breach indicates that Defendant failed to adequately implement one or more of the above measures to prevent cyberattacks, resulting in the Data Breach and data thieves acquiring and accessing the PII of more than 70,000 individuals, including that of Plaintiffs and Class members.

140. Defendant acquires, collects, and stores a massive amount of PII on its current and former customers.

141. As a condition of obtaining services from Defendant, Defendant requires that

[5] *Id.* at 3-4.

customers and other personnel entrust it with highly sensitive personal information.

142. By obtaining, collecting, and using Plaintiffs' and Class Members' PII, Defendant assumed legal and equitable duties and knew or should have known that it was responsible for protecting Plaintiffs' and Class Members' PII from disclosure.

D. Defendant Knew or Should Have Known of the Risk of Data Breaches Because Financial Institutions in Possession of PII Are Particularly Susceptible to Cyber Attacks

143. Defendant's data security obligations were particularly important given the substantial increase in cyber attacks and/or data breaches targeting financial institutions that collect and store PII, like Defendant, preceding the data of the Data Breach.

144. In light of recent high profile data breaches at other industry leading companies, including National Public Data (2.9 billion records, August 2024), Ticketmaster Entertainment, LLC (560 million records, May 2024), Change Healthcare Inc. (145 million records, February 2024), Dell Technologies, Inc. (49 million records, May 2024), and AT&T Inc. (73 million records, April 2024), Defendant knew or should have known that the PII they collected and maintained would be targeted by cybercriminals.

145. Plaintiffs and Class members now face years of constant surveillance of their financial and personal records. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

146. As a financial institution in custody of the PII of its customers, Defendant knew, or should have known, the importance of safeguarding PII entrusted to it by Plaintiff and Class members, and of the foreseeable consequences if its data security systems were breached. This includes the significant costs imposed on Plaintiffs and Class Members as a result of a breach. Defendant failed, however, to take adequate cybersecurity measures to prevent the Data Breach.

E. The Value of Personally Identifying Information

147. The Federal Trade Commission ("FTC") defines identity theft as "a fraud committed or attempted using the identifying information of another person without authority."[6] The FTC describes "identifying information" as "any name or number that may be used, alone or in conjunction with any other information, to identify a specific person," including, among other things, "[n]ame, Social Security number, date of birth, official State or government issued driver's license or identification number, alien registration number, government passport number, employer or taxpayer identification number."[7]

148. The PII of individuals remains of high value to criminals, as evidenced by the prices they will pay through the dark web. Numerous sources cite dark web pricing for stolen identity credentials.[8] For example, PII can be sold at prices ranging from $40 to $200.[9] Criminals can also purchase access to entire company data breaches at prices ranging from $900 to $4,500.[10]

149. Of course, a stolen Social Security number – standing alone – can be used to wreak untold havoc upon a victim's personal and financial life. A thief can use a person's Social Security number for the purposes of financial identity theft, government identity theft, criminal identity theft, medical identity theft, and utility fraud.[11] Social Security numbers are among the worst kind of PII to have stolen because they may be put to a variety of fraudulent uses and are difficult for

[6] 17 C.F.R. § 248.201 (2013).
[7] *Id.*
[8] Anita George, *Your personal data is for sale on the dark web. Here's how much it costs,* DIGITAL TRENDS (Oct. 16, 2019), https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/.
[9] Brian Stack, *Here's How Much Your Personal Information Is Selling for on the Dark Web*, EXPERIAN (Dec. 6, 2017), https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/.
[10] *In the Dark*, VPNOVERVIEW (2019), https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/.
[11] Alison Grace Johansen, *5 Kinds of ID Theft Using a Social Security Number*, LIFELOCK BY NORTON (Nov. 30, 2017), https://lifelock.norton.com/learn/identity-theft-resources/kinds-of-id-theft-using-social-security-number.

an individual to change.

150. What's more, it is no easy task to change or cancel a stolen Social Security number. An individual cannot obtain a new Social Security number without significant paperwork and evidence of actual misuse. In other words, preventive action to defend against the possibility of misuse of a Social Security number is not permitted; an individual must show evidence of actual, ongoing fraud activity to obtain a new number.

151. Even then, a new Social Security number may not be an effective defense against further theft, because "[t]he credit bureaus and banks are able to link the new number very quickly to the old number, so all of that old bad information is quickly inherited into the new Social Security number."[12]

152. Based on the foregoing, the information compromised in the Data Breach is significantly more valuable than the loss of, for example, credit card information in a retailer data breach. Where victims of credit card theft have the option to cancel or close credit and debit card accounts, the information compromised in this Data Breach is impossible to "close" and difficult, if not impossible, to change.

153. The fraudulent activity resulting from the Data Breach may not come to light for years. There may be a time lag between when harm occurs versus when it is discovered, and also between when PII is stolen and when it is used.

154. Plaintiffs and Class Members now face years of constant surveillance of their financial and personal records. The Class is incurring and will continue to incur such damages in addition to any fraudulent use of their PII.

[12] Bryan Naylor, *Victims of Social Security Number Theft Find It's Hard to Bounce Back*, NPR (Feb. 9, 2015), http://www.npr.org/2015/02/09/384875839/data-stolen-by-anthem-s-hackers-has-millionsworrying-about-identity-theft.

F. Defendant Failed to Comply with Federal Trade Commission ("FTC") Guidelines

155. The FTC has promulgated numerous guides for businesses which highlight the importance of implementing reasonable data security practices. According to the FTC, the need for data security should be factored into all business decision-making.

156. In 2016, the FTC updated its publication, Protecting Personal Information: A Guide for Business, which established cyber security guidelines for businesses.[13] These guidelines note that businesses should protect the personal consumer information that they keep, properly dispose of personal information that is no longer needed, encrypt information stored on computer networks, understand their network's vulnerabilities, and implement policies to correct any security problems.[14]

157. The guidelines also recommend that businesses use an intrusion detection system to expose a breach as soon as it occurs, monitor all incoming traffic for activity indicating someone is attempting to hack the system, watch for large amounts of data being transmitted from the system, and have a response plan ready in the event of a breach.[15]

158. The FTC further recommends that companies not maintain PII longer than is needed for authorization of a transaction, limit access to sensitive data, require complex passwords to be used on networks, use industry-tested methods for security, monitor for suspicious activity on the network, and verify that third-party service providers have implemented reasonable security measures.[16]

159. The FTC regularly brings enforcement actions against businesses for failing to

[13] *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.
[14] *Id.*
[15] *Id.*
[16] *Id.*

adequately and reasonably protect consumer data, treating the failure to employ reasonable and appropriate measures to protect against unauthorized access to confidential consumer data as an unfair act or practice prohibited by Section 5 of the Federal Trade Commission Act ("FTCA"), 15 U.S.C. § 45.[17] Orders resulting from these actions further clarify the measures businesses must take to meet their data security obligations.

160. The FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendant, of failing to use reasonable measures to protect PII.[18] The FTC publications and orders described above also form part of the basis of Defendant's duty in this regard.

161. Defendant failed to properly implement basic data security practices.

162. Defendant's failure to employ reasonable and appropriate measures to protect against unauthorized access to the PII of its customers or to comply with applicable industry standards constitutes an unfair act or practice prohibited by Section 5 of the FTCA, 15 U.S.C. § 45.

163. Upon information and belief, Defendant was at all times fully aware of its obligation to protect the PII of its customers and the significant repercussions that would result from its failure to do so. Accordingly, Defendant's conduct was particularly unreasonable given the nature and amount of PII it obtained and stored and the foreseeable consequences of the immense damages that would result to Plaintiffs and the Class.

---

[17] *See, e.g.*, *Enforcement*, FEDERAL TRADE COMMISSION, https://www.ftc.gov/enforcement (last visited May 27, 2025).

[18] *See, e.g.,* 15 U.S.C. § 45; *Protecting Personal Information: A Guide for Business*, FEDERAL TRADE COMMISSION (2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

G. Defendant Failed to Comply with the Gramm-Leach-Bliley Act ("GLBA")

164. Defendant is a financial institution as that term is defined by the GLBA, 15 U.S.C. § 6809(3)(A), and thus is subject to the GLBA.

165. The GLBA defines a financial institution as "any institution the business of which is engaging in financial activities as described in Section 1843(k) of Title 12 [The Bank Holding Company Act of 1956]." 15 U.S.C. § 6809(3)(A).

166. Defendant collects nonpublic personal information, as defined by 15 U.S.C. § 6809(4)(A), 16 C.F.R. § 313.3(n), and 12 C.F.R. § 1016.3(p)(1). Accordingly, during the relevant time period, Defendant was subject to the requirements of the GLBA, 15 U.S.C. §§ 6801.1, *et seq*., and is still subject to numerous rules and regulations promulgated on the GLBA statutes.

167. The GLBA Privacy Rule became effective on July 1, 2001. *See* 16 C.F.R. Part 313. Since the enactment of the Dodd-Frank Act on July 21, 2010, the Consumer Financial Protection Bureau ("CFPB") is responsible for implementing the GLBA Privacy Rule. In December 2011, the CFPB restated the implementing regulations in an interim final rule that established the Privacy of Consumer Financial Information, Regulation P, 12 C.F.R. § 1016 ("Regulation P"), with the final version becoming effective on October 28, 2014.

168. Accordingly, Defendant's conduct is governed by the Privacy Rule prior to December 30, 2011, and by Regulation P after that date.

169. Both the Privacy Rule and Regulation P require financial institutions to provide customers with an initial and annual privacy notice. These privacy notices must be "clear and conspicuous." 16 C.F.R. §§ 313.4-313.5; 12 C.F.R. §§ 1016.4-1016.5. "Clear and conspicuous means that a notice is reasonably understandable and designed to call attention to the nature and significance of the information in the notice." 16 C.F.R. § 313.3(b)(1); 12 C.F.R. § 1016.3(b)(1).

These privacy notices must "accurately reflect[] [the financial institution's] privacy policies and practices." 16 C.F.R. § 313.4-313.5; 12 C.F.R. §§ 1016.4-1016.5. The privacy notices must include specified elements, including: (1) the categories of nonpublic personal information the financial institution collects and discloses; (2) the categories of third parties to whom the financial institution discloses the information; and (3) the financial institution's security and confidentiality policies and practices for nonpublic personal information. 16 C.F.R. § 313.6; 12 C.F.R. § 1016.6. These privacy notices must be provided "so that each consumer can reasonably be expected to receive actual notice." 16 C.F.R. § 313.9; 12 C.F.R. § 1016.9. As alleged herein, Defendant violated the Privacy Rule and Regulation P.

170. Upon information and belief, Defendant failed to provide annual privacy notices to customers after the customer relationship ended, despite retaining these customers' PII and storing that PII on Defendant's network systems.

171. Defendant failed to adequately inform their customers that they were storing and/or sharing, or would store and/or share, the customers' PII on an insecure platform, accessible to unauthorized parties from the internet, and would do so after the customer relationship ended.

172. The Safeguards Rule, which implements Section 501(b) of the GLBA, 15 U.S.C. § 6801(b), requires financial institutions to protect the security, confidentiality, and integrity of customer information by developing a comprehensive written information security program that contains reasonable administrative, technical, and physical safeguards, including: (1) designating one or more employees to coordinate the information security program; (2) identifying reasonably foreseeable internal and external risks to the security, confidentiality, and integrity of customer information, and assessing the sufficiency of any safeguards in place to control those risks; (3) designing and implementing information safeguards to control the risks identified through risk

assessment, and regularly testing or otherwise monitoring the effectiveness of the safeguards' key controls, systems, and procedures; (4) overseeing service providers and requiring them by contract to protect the security and confidentiality of customer information; and (5) evaluating and adjusting the information security program in light of the results of testing and monitoring, changes to the business operation, and other relevant circumstances. 16 C.F.R. §§ 314.3-314.4.

173. As alleged herein, Defendant violated the Safeguard Rule.

174. Defendant failed to assess reasonably foreseeable risks to the security, confidentiality, and integrity of customer information and failed to monitor the systems of its IT partners or verify the integrity of those systems.

175. Defendant violated the GLBA and its own policies and procedures by sharing the PII of Plaintiffs and Class members with a non-affiliated third party without providing Plaintiffs and Class members (a) an opt-out notice and (b) a reasonable opportunity to opt out of such disclosure.

H. Defendant Failed to Comply with Industry Standards

176. As noted above, experts studying cyber security routinely identify financial institutions in possession of PII as being particularly vulnerable to cyberattacks because of the value of the PII which they collect and maintain.

177. Several best practices have been identified that, at a minimum, should be implemented by financial institutions in possession of PII, like Defendant. These best practices include but are not limited to: (1) educating all employees; (2) requiring strong passwords; (3) implementing multi-layer security, including firewalls, anti-virus, and anti-malware software; (4) encryption, (5) making data unreadable without a key; (6) multi-factor authentication; (7) backup data; (8) limiting which employees can access sensitive data; (9) installing appropriate malware

detection software; (10) monitoring and limiting the network ports; (11) protecting web browsers and email management systems; (12) setting up network systems such as firewalls, switches, and routers; (13) monitoring and protection of physical security systems; (14) protection against any possible communication system; and (15) training staff regarding critical points. Defendant failed to follow these industry best practices.

178. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 2.0 (including, without limitation, PR.AA-01, PR.AA.-02, PR.AA-03, PR.AA-04, PR.AA-05, PR.AT-01, PR.DS-01, PR-DS-02, PR.DS-10, PR.PS-01, PR.PS-02, PR.PS-05, PR.IR-01, DE.CM-01, DE.CM-03, DE.CM-06, DE.CM-09, and RS.CO-04), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

179. These foregoing frameworks are existing and applicable industry standards for financial institutions. Upon information and belief, Defendant failed to comply with at least one––or all—of these accepted standards, thereby opening the door to the threat actor and causing the Data Breach.

180. Unencrypted PII may also fall into the hands of companies that will use the detailed PII for targeted marketing without the approval of Plaintiffs and Class Members.

181. The link between a data breach and the risk of identity theft is simple and well-established. Criminals acquire and steal PII to monetize the information by selling the stolen information on the black market to other criminals, who then utilize the information to commit a variety of identity theft related crimes discussed below.

182. State legislatures have passed laws in recognition of the risks associated with stolen Social Security numbers: "[t]he [S]ocial [S]ecurity number can be used as a tool to perpetuate

fraud against a person and to acquire sensitive personal, financial, medical, and familial information, the release of which could cause great financial or personal harm to an individual. While the [S]ocial [S]ecurity number was intended to be used solely for the administration of the federal Social Security System, over time this unique numeric identifier has been used extensively for identity verification purposes[.]"[19]

183. Moreover, "SSNs have been central to the American identity infrastructure for years, being used as a key identifier[.] . . . U.S. banking processes have also had SSNs baked into their identification process for years. In fact, SSNs have been the gold standard for identifying and verifying the credit history of prospective customers."[20]

184. "Despite the risk of fraud associated with the theft of Social Security numbers, just five of the nation's largest 25 banks have stopped using the numbers to verify a customer's identity after the initial account setup[.]"[21] Accordingly, since Social Security numbers are frequently used to verify an individual's identity after logging onto an account or attempting a transaction, "[h]aving access to your Social Security number may be enough to help a thief steal money from your bank account."[22]

185. One such example of criminals piecing together portions of compromised PII for profit is the development of "Fullz" packages.[23]

---

[19] *See* N.C. Gen. Stat. § 132-1.10(a)(1).

[20] Husayn Kassai*, Banks need to stop relying on social security numbers,* AMERICAN BANKER (Nov. 12, 2018, 10:07 AM) https://www.americanbanker.com/opinion/banks-need-to-stop-relying-on-social-security-numbers.

[21] Ann Carrns, *Just 5 Banks Prohibit Use of Social Security Numbers*, THE NEW YORK TIMES (Mar. 20, 2013, 10:59 AM) https://archive.nytimes.com/bucks.blogs.nytimes.com/2013/03/20/just-5-banks-prohibit-use-of-social-security-numbers/.

[22] Nikkita Walker, *What Can Someone Do With Your Social Security Number?*, CREDIT.COM (Oct. 19, 2023), https://www.credit.com/blog/5-things-an-identity-thief-can-do-with-your-social-security-number-108597/.

[23] "Fullz" is fraudster speak for data that includes the information of the victim, including, but not limited to, the name, address, credit card information, Social Security number, date of birth, and more. As a rule of thumb, the more information you have about a victim, the more money that can be made off of those

186. With "Fullz" packages, cyber-criminals can cross-reference two sources of PII to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete dossiers on individuals.

187. In this case, the development of "Fullz" packages means that the stolen PII from the Data Breach can easily be used to link and identify it to Plaintiffs' and Class Members' phone numbers, email addresses, and other unregulated sources and identifiers. In other words, even if certain information such as emails, phone numbers, or credit card numbers may not be included in the PII that was exfiltrated in the Data Breach, criminals may still easily create a Fullz package and sell it at a higher price to unscrupulous operators and criminals (such as illegal and scam telemarketers) over and over.

188. The existence and prevalence of "Fullz" packages means that the PII stolen from the Data Breach can easily be linked to the unregulated data, such as contact information, of Plaintiffs and the other Class Members. Thus, even if certain information was not stolen in the data breach, criminals can still easily create a comprehensive "Fullz" package. Then, this comprehensive dossier can be sold—and then resold in perpetuity—to crooked operators and other criminals.

I. Loss of Time to Mitigate Risk of Identity Theft and Fraud

189. As a result of the recognized risk of identity theft, when a data breach occurs and

credentials. Fullz are usually pricier than standard credit card credentials, commanding up to $100 per record (or more) on the dark web. Fullz can be cashed out (turning credentials into money) in various ways, including performing bank transactions over the phone with the required authentication details in-hand. Even "dead Fullz," which are Fullz credentials associated with credit cards that are no longer valid, can still be used for numerous purposes, including tax refund scams, ordering credit cards on behalf of the victim, or opening a "mule account" (an account that will accept a fraudulent money transfer from a compromised account) without the victim's knowledge. *See*, *e.g.*, Brian Krebs, *Medical Records for Sale in Underground Stolen From Texas Life Insurance Firm*, KREBS ON SECURITY (Sep. 18, 2014), https://krebsonsecurity.com/2014/09/medical-records-for-sale-in-underground-stolen-from-texas-life-insurance-firm/.

an individual is notified by a company that their PII was compromised, as in this Data Breach, the reasonable person is expected to take steps and spend time to address the dangerous situation, learn about the breach, and otherwise mitigate the risk of becoming a victim of identity theft of fraud. Failure to spend time taking steps to review accounts or credit reports could expose the individual to greater financial harm.

190. Thus, Defendant, in its Notice Letter, instructs Class members to "remain vigilant to protect against potential fraud and/or identity theft by, among other things, reviewing your account statements and monitoring credit reports closely."[24]

191. Plaintiffs and Class members have spent, and will spend additional time in the future, on a variety of prudent actions, such as researching and verifying the legitimacy of the Data Breach and monitoring their financial and personal accounts. Accordingly, the Data Breach has caused Plaintiffs and Class members to suffer actual injury in the form of lost time spent on mitigation activities. This time cannot be recaptured.

192. Plaintiffs' mitigation efforts are consistent with the 2007 U.S. Government Accountability Office report regarding data breaches ("GAO Report"), in which it noted that victims of identity theft will face "substantial costs and time to repair the damage to their good name and credit record."[25]

J. Diminution of Value of PII

193. PII is a valuable property right.[26] Its value is axiomatic, demonstrated through the value of Big Data in corporate America and the legal consequences of cyber thefts, including long

[24] *Id.*
[25] *See* United States Government Accountability Office, *GAO-07-737, Personal Information: Data Breaches Are Frequent, but Evidence of Resulting Identity Theft Is Limited; However, the Full Extent Is Unknown* (June 2007), https://www.gao.gov/new.items/d07737.pdf.
[26] *Id.* at 2.

prison sentences.

194. An active and robust marketplace for PII exists. Sensitive PII can sell for as much as $363 per record according to the Infosec Institute.[27] In 2019, the data brokering industry was worth roughly $200 billion.[28]

195. In fact, the data marketplace is so sophisticated that consumers can sell their non-public information directly to a data broker, who in turn aggregates the information and provides it to marketers or app developers.[29]

K. Future Cost of Credit and Identity Theft Monitoring

196. Given the targeted attack, sophisticated criminal activity, and the type of PII involved in this case, there is a strong probability that entire batches of stolen information have been placed, or will be placed, on the black market/dark web for sale and purchase by criminals intending to utilize the PII for identity theft crimes, such as opening bank accounts in the victims' names to make purchases or launder money, filing false tax returns, taking out loans or lines of credit, or filing false unemployment claims.

197. Such fraud may go undetected until debt collection calls commence months, or even years, later. An individual may not know that their PII was used to file for unemployment benefits until law enforcement notifies the individual's employer of the suspected fraud. Fraudulent tax returns are typically discovered only when an individual's authentic tax return is rejected.

---

[27] *See, e.g.,* John T. Soma, et al, *Corporate Privacy Trend: The "Value" of Personally Identifiable Information ("PII") Equals the "Value" of Financial Assets*, 15 RICH. J.L. & TECH. 11, at *3-4 (2009) ("PII, which companies obtain at little cost, has quantifiable value that is rapidly reaching a level comparable to the value of traditional financial assets.") (citations omitted).

[28] *See* Ashiq Ja, *Hackers Selling Healthcare Data in the Black Market*, INFOSEC (July 27, 2015), https://resources.infosecinstitute.com/topic/hackers-selling-healthcare-data-in-the-black-market/.

[29] David Lazarus, *Shadowy data brokers make the most of their invisibility cloak,* LOS ANGELES TIMES (Nov. 5, 2019, 5:00 PM) https://www.latimes.com/business/story/2019-11-05/column-data-brokers. *See also* DATA COUP, https://datacoup.com/ (last visited May 27, 2025).

Consequently, Plaintiffs and Class members are at an increased risk of fraud and identity theft for many years into the future.

L. Loss of Benefit of the Bargain

198. Furthermore, Defendant's poor data security practices deprived Plaintiffs and Class members of the benefit of their bargain. When agreeing to pay Defendant and/or its agents for services, Plaintiffs and other reasonable consumers understood and expected that they were, in part, paying for the product and/or service and necessary data security to protect the PII, when in fact, Defendant did not provide the expected data security. Accordingly, Plaintiffs and Class members received services that were of a lesser value than what they reasonably expected to receive under the bargains they struck with Defendant.

V. CLASS ACTION ALLEGATIONS

199. Plaintiffs bring this nationwide class action on behalf of themselves and on behalf of all others similarly situated, as referred to throughout this Complaint as "the Class" and "Class members."

200. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiffs propose the following Nationwide Class definition:

> **Nationwide Class**: All persons in the United States whose PII was compromised as a result of the Data Breach reported by Defendant in March 2025.

201. Pursuant to Rule 23 of the Federal Rules of Civil Procedure, Plaintiffs propose the following State Subclass definitions, subject to amendment as appropriate:

> **California Subclass**: All persons in the state of California whose PII was compromised as a result of the Data Breach reported by Defendant in March 2025.

202. Excluded from the Class are the following individuals and/or entities: Defendant and Defendant's parents, subsidiaries, affiliates, officers and directors, and any entity in which Defendant have a controlling interest; all individuals who make a timely election to be excluded

from this proceeding using the correct protocol for opting out; and all judges assigned to hear any aspect of this litigation, as well as their immediate family members.

203. **Numerosity**. The members of the Class are so numerous that joinder of all members is impracticable, if not completely impossible. According to the Data Breach report submitted to the Office of the Maine Attorney General, approximately 75,000 persons were impacted in the Data Breach.[30]

204. **Commonality**. Common questions of law and fact exist as to all members of the Class and predominate over any questions affecting solely individual members of the Class. These common questions of law and fact include, without limitation:

a. Whether and to what extent Defendant had a duty to protect the PII of Plaintiffs and Class members;

b. Whether Defendant had respective duties not to disclose the PII of Plaintiffs and Class members to unauthorized third parties;

c. Whether Defendant had respective duties not to use the PII of Plaintiffs and Class members for non-business purposes; and,

d. Whether Defendant failed to adequately safeguard the PII of Plaintiffs and Class members.

205. **Typicality**. Plaintiffs' claims are typical of those of the other members of the Class because Plaintiffs, like every other Class member, were exposed to virtually identical conduct and now suffer from the same violations of the law as each other member of the Class.

206. **Policies Generally Applicable to the Class**. This class action is also appropriate for certification because Defendant acted or refused to act on grounds generally applicable to the Class, thereby requiring the Court's imposition of uniform relief to ensure compatible standards

[30] *Data Breach Notifications*, OFFICE OF THE MAINE ATTORNEY GENERAL, https://www.maine.gov/agviewer/content/ag/985235c7-cb95-4be2-8792-a1252b4f8318/6c038d1f-41db-4c57-9bdd-c1c7215b7eba.html (last visited May 27, 2025).

of conduct toward the Class members and making final injunctive relief appropriate with respect to the Class as a whole.

207. **Adequacy.** Plaintiffs will fairly and adequately represent and protect the interests of the Class members in that they have no disabling conflicts of interest that would be antagonistic to those of the other Class members. Plaintiffs seek no relief that is antagonistic or adverse to the Class members and the infringement of the rights and the damages they have suffered are typical of other Class members.

208. **Superiority and Manageability.** The class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class action treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein; it will permit a large number of Class members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require.

VI. CAUSES OF ACTION

COUNT I
Negligence
(On Behalf of Plaintiffs and the Class)

209. Plaintiffs re-allege and incorporate by reference all of the allegations contained in all the above paragraphs, as though fully set forth herein.

210. Defendant requires its customers, including Plaintiffs and Class members, to submit non-public PII in the ordinary course of providing its services. Defendant gathered and stored the PII of Plaintiffs and Class members as part of its business of soliciting its services to its customers.

211. Plaintiffs and Class members entrusted Defendant with their PII with the understanding that Defendant would safeguard their information.

212. Defendant had full knowledge of the sensitivity of the PII and the types of harm

that Plaintiffs and Class members could and would suffer if the PII were wrongfully disclosed.

213. By voluntarily undertaking and assuming the responsibility to collect and store this data and sharing it and using it for commercial gain, Defendant owed a duty of care not to subject Plaintiffs' and Class members' PII to an unreasonable risk of exposure and theft. Plaintiffs and the Class members were foreseeable and probable victims of any inadequate security practices.

214. Defendant owed numerous duties to Plaintiffs and the Class, including the following:

a. to exercise reasonable care in obtaining, retaining, securing, safeguarding, deleting, and protecting Private Information in their possession;

b. to protect Private Information using reasonable and adequate security systems that are compliant with industry-standard practices, the FTCA, and the GLBA[31]; and

c. to implement processes to quickly detect a data breach, timely act on warnings about data breaches, and promptly and adequately notify customers about data breaches.

215. Defendant also breached its duty to Plaintiffs and the Class members to adequately protect and safeguard Private Information by disregarding standard information security principles, despite obvious risks, and by allowing unmonitored and unrestricted access to unsecured Private Information. Furthering their dilatory practices, Defendant failed to provide adequate supervision and oversight of the Private Information with which they were and are entrusted, in spite of the known risk and foreseeable likelihood of breach and misuse, which permitted a malicious third party to gather Plaintiffs' and Class members' Private Information and potentially misuse the Private Information and intentionally disclose it to others without consent.

[31] Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data. 15 U.S.C. § 6809(3)(A).

216. Defendant knew, or should have known, of the risks inherent in collecting and storing Private Information and the importance of adequate security. Defendant knew or should have known about numerous well-publicized data breaches within the financial industry.

217. Defendant knew, or should have known, that their data systems and networks did not adequately safeguard Plaintiffs' and Class members' Private Information.

218. Defendant breached their duties to Plaintiffs and the Class members by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' Private Information.

219. Because Defendant knew that a breach of their systems would damage thousands of their customers, including Plaintiffs and the Class members, Defendant had a duty to adequately protect their data systems and the Private Information contained thereon.

220. Defendant's duty of care to use reasonable security measures arose as a result of the special relationship that existed between Defendant and their clients, which is recognized by laws and regulations including but not limited to common law. Defendant was in a position to ensure that their systems were sufficient to protect against the foreseeable risk of harm to Class members from a data breach.

221. In addition, Defendant had a duty to employ reasonable security measures under Section 5 of the Federal Trade Commission Act, 15 U.S.C. § 45, which prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair practice of failing to use reasonable measures to protect confidential data.

222. Defendant's duty to use reasonable care in protecting confidential data arose not only as a result of the statutes and regulations described above, but also because Defendant is bound by industry standards to protect confidential Private Information.

223. Defendant's own conduct also created a foreseeable risk of harm to Plaintiffs and Class members and their Private Information. Defendant's misconduct included failing to: (1) secure Plaintiffs' and the Class members' Private Information; (2) comply with industry standard security practices; (3) implement adequate system and event monitoring; and (4) implement the systems, policies, and procedures necessary to prevent this type of data breach.

224. Defendant breached their duties, and thus were negligent, by failing to use reasonable measures to protect Class members' Private Information, and by failing to provide timely notice of the Data Breach. The specific negligent acts and omissions committed by Defendant include, but are not limited to, the following:

a. Failing to adopt, implement, and maintain adequate security measures to safeguard Class members' Private Information;

b. Failing to adequately monitor the security of Defendant's networks and systems;

c. Allowing unauthorized access to Class members' Private Information;

d. Failing to detect in a timely manner that Class members' Private Information had been compromised; and

e. Failing to timely notify Class members about the Security Breach so that they could take appropriate steps to mitigate the potential for identity theft and other damages.

225. Through Defendant's acts and omissions described in this Complaint, including their failure to provide adequate security and their failure to protect Plaintiffs' and Class members' Private Information from being foreseeably captured, accessed, disseminated, stolen and misused, Defendant unlawfully breached its duty to use reasonable care to adequately protect and secure Plaintiffs' and Class members' Private Information during the time it was within Defendant's possession or control.

226. Defendant's conduct was grossly negligent and departed from all reasonable standards of care, including, but not limited to: failing to adequately protect the Private Information and failing to provide Plaintiffs and Class members with timely notice that their sensitive Private Information had been compromised.

227. Neither Plaintiffs nor the other Class members contributed to the Data Breach and subsequent misuse of their Private Information as described in this Complaint.

228. As a direct and proximate cause of Defendant's conduct, Plaintiffs and Class members suffered damages as alleged above.

229. Plaintiff and Class members are also entitled to injunctive relief requiring Defendant to, e.g., (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide lifetime free credit monitoring to all Class members.

COUNT II
Breach of Implied Contract
(On Behalf of Plaintiffs and the Class)

230. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

231. Defendant solicited and invited Class members or other entities working on their behalf to provide their Private Information as part of Defendant's regular business practices. When Plaintiffs and Class members or other entities operating on their behalf made and paid for purchases of Defendant's services and products, they provided their Private Information to Defendant.

232. In so doing, Plaintiffs and Class members entered into implied contracts with Defendant pursuant to which Defendant agreed to safeguard and protect such information and to

timely detect any breaches of their Private Information. In entering into such implied contracts, Plaintiffs and Class members reasonably believed and expected that Defendant's data security practices complied with relevant laws and regulations, and were consistent with industry standards.

233. Class members reasonably believed and expected that Defendant would use part of those funds to obtain adequate data security. Defendant failed to do so.

234. Plaintiffs and Class members would not have provided and entrusted their Private Information with Defendant in the absence of the implied contract between them and Defendant.

235. Plaintiffs and Class members fully performed their obligations under the implied contracts with Defendant.

236. Defendant breached the implied contracts they made with Plaintiffs and Class members by failing to safeguard and protect their Private Information and by failing to timely detect the data breach within a reasonable time.

237. As a direct and proximate result of Defendant's breaches of the implied contracts between Defendant, Plaintiffs, and Class members, Plaintiffs and Class members sustained actual losses and damages as described in detail above.

238. Plaintiffs and Class members are also entitled to injunctive relief requiring Defendant to, *e.g.*, (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide free lifetime credit monitoring to all Class members.

COUNT III
Unjust Enrichment
(On Behalf of Plaintiffs and the Class)

239. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

240. Plaintiffs and Class members conferred a monetary benefit on Defendant. Specifically, they or other entities operating on their behalf purchased goods and services from Defendant and provided Defendant with their Private Information. In exchange, Plaintiffs and Class members should have received from Defendant the goods and services that were the subject of the transaction and should have been entitled to have Defendant protect their Private Information with adequate data security.

241. Defendant knew that Plaintiffs and Class members conferred a benefit on them and accepted or retained that benefit. Defendant profited from this and used Plaintiffs' and the Class members' Private Information for business purposes.

242. Defendant failed to secure Plaintiffs' and the Class members' Private Information and, therefore, did not provide full compensation for the benefit of the Plaintiffs' and Class members' Private Information provided.

243. Defendant acquired the Private Information through inequitable means as they failed to disclose the inadequate security practices previously alleged.

244. If Plaintiffs and the Class members knew that Defendant would not secure their Private Information using adequate security, they would not have allowed entities to entrust Defendant with their Personal Information.

245. Plaintiffs and Class members have no adequate remedy at law.

246. Under the circumstances, it would be unjust for Defendant to be permitted to retain any of the benefits that Plaintiffs and Class members conferred on them.

247. Defendant should be compelled to disgorge into a common fund or constructive trust, for the benefit of Plaintiffs and Class members, proceeds that they unjustly received from

them. In the alternative, Defendant should be compelled to refund the amounts that Plaintiffs and Class members overpaid.

COUNT IV
Negligence Per Se
(On Behalf of Plaintiffs and the Class)

248. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

249. Pursuant to the FTCA, 15 U.S.C. § 45, Defendant had a duty to provide fair and adequate computer systems and data security practices to safeguard Plaintiffs' and Class members' PII.

250. The FTC publications and orders promulgated pursuant to the FTCA also form part of the basis of Defendant's duty to protect Plaintiffs' and Class members' sensitive Private Information. Section 5 of the FTCA prohibits "unfair . . . practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as LFCU, of failing to use reasonable measures to protect clients' PII.

251. Defendant violated its duty under Section 5 of the FTCA by failing to use reasonable measures to protect its clients' PII and by failing to comply with applicable industry standards as described in detail herein. Defendant's conduct was particularly unreasonable given the nature and amount of PII LFCU had collected and stored and the foreseeable consequences of a data breach, including the immense damages that would result to its clients in the event of a breach, which ultimately came to pass.

252. The harm that has occurred is the type of harm the FTCA is intended to guard against. Indeed, the FTC has pursued numerous enforcement actions against businesses that, because of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and members of the Class.

253. Defendant had a duty to Plaintiffs and the Class to implement and maintain reasonable security procedures and practices to safeguard their PII.

254. Defendant breached their duties to Plaintiffs and members of the Class under the FTCA by failing to provide fair, reasonable, or adequate computer systems and data security practices to safeguard Plaintiffs and Class members' PII.

255. Defendant's violation of Section 5 of the FTCA and its failure to comply with applicable laws and regulations constitutes negligence per se.

256. But for Defendant's wrongful and negligent breach of their duties owed to Plaintiffs and members of the Class, Plaintiffs and members of the Class would not have been injured.

257. The injury and harm suffered by Plaintiffs and members of the Class were the reasonably foreseeable result of Defendant's breach of their duties. Defendant knew or should have known that it was failing to meet its duties and that its breach would cause Plaintiffs and the Class to suffer the foreseeable harms associated with the exposure of their PII.

258. Had Plaintiffs and members of the Class known that Defendant did not adequately protect the PII entrusted to it, Plaintiffs and members of the Class would not have entrusted LFCU with their PII.

259. As a direct and proximate result of Defendant's negligence per se, Plaintiffs and members of the Class have suffered harm, including, but not limited to, loss of time and money resolving fraudulent charges; loss of time and money obtaining protections against future identity theft; financial losses related to the treatment Plaintiffs and members of the Class paid for that they would not have sought had they known of Defendant's careless approach to cyber security; lost control over the use of their PII; unreimbursed losses relating to fraudulent charges; harm resulting from damaged credit scores and information; and other harm resulting from the

unauthorized use or threat of unauthorized use of stolen personal information, entitling them to damages in an amount to be proven at trial.

COUNT V
Breach of Fiduciary Duty
(On Behalf of Plaintiffs and the Class)

260. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

261. In providing their PII, directly or indirectly, to Defendant, Plaintiffs and Class members justifiably placed a special confidence in Defendant to act in good faith and with due regard to interests of Plaintiffs and Class members to safeguard and keep confidential that PII.

262. Defendant accepted the special confidence Plaintiffs and Class members placed in it, as evidenced by its assertion that it is committed to protecting the privacy of Plaintiffs' and Class members' personal information as detailed in its Privacy Policy.

263. In light of the special relationship between Defendant and Plaintiffs and Class members, whereby Defendant became a guardian of Plaintiffs' and Class members' PII, Defendant became a fiduciary by its undertaking and guardianship of the PII, to act primarily for the benefit of its customers, including Plaintiffs and Class members, for the safeguarding of Plaintiffs' and Class members' PII.

264. Defendant has a fiduciary duty to act for the benefit of Plaintiffs and Class members upon matters within the scope of its relationship with Defendants' customers—in particular, to keep the PII of its customers secure.

265. Defendant breached its fiduciary duties to Plaintiffs and Class members by failing to protect the integrity of the systems containing Plaintiffs' and Class members' PII.

266. Defendant breached its fiduciary duties to Plaintiffs and Class members by otherwise failing to safeguard Plaintiffs' and Class members' PII.

267. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class members have suffered and will suffer injury, including but not limited to: (i) invasion of privacy; (ii) lost or diminished value of PII; (iii) lost time and opportunity costs associated with attempting to mitigate the actual consequences of the Data Breach; (iv) loss of benefit of the bargain; and (v) the continued and certainly increased risk to their PII, which: (a) remains unencrypted and available for unauthorized third parties to access and abuse; and (b) remains backed up in Defendant's possession and is subject to further unauthorized disclosures so long as Defendant fails to undertake appropriate and adequate measures to protect the PII.

268. As a direct and proximate result of Defendant's breaches of its fiduciary duties, Plaintiffs and Class members have suffered and will continue to suffer other forms of injury and/or harm, and other economic and non-economic losses.

COUNT VI
Invasion of Privacy
(On behalf of Plaintiffs and the Class)

269. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

270. Plaintiffs and Class members had a legitimate expectation of privacy regarding their PII and were accordingly entitled to the protection of this information against disclosure to unauthorized third parties.

271. Defendant owed a duty to Plaintiffs and Class members to keep their PII confidential.

272. The unauthorized disclosure and/or acquisition (*i.e.,* theft) by a third party of Plaintiffs' and Class members' PII is highly offensive to a reasonable person.

273. Defendant's reckless and negligent failure to protect Plaintiffs' and Class members' PII constitutes an intentional interference with Plaintiffs' and the Class members'

interest in solitude or seclusion, either as to their person or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

274. Defendant acted with knowledge when it failed to protect Plaintiffs' and Class members' PII because it knew its information security practices were inadequate.

275. Defendant knowingly did not notify Plaintiffs and Class members about the Data Breach in a timely fashion.

276. Because Defendant failed to properly safeguard Plaintiffs' and Class members' PII, Defendant had notice that its inadequate cybersecurity practices would cause injury to Plaintiffs and the Class.

277. As a proximate result of Defendant's acts and omissions, the private and sensitive PII of Plaintiffs and the Class Members was stolen by a third party and is now available for disclosure and redisclosure without authorization, causing Plaintiffs and the Class to suffer damages.

278. Defendant's wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and the Class since their PII is still maintained by Defendant with their inadequate cybersecurity system and policies.

279. Plaintiffs and Class Members have no adequate remedy at law for the injuries relating to Defendant's continued possession of their sensitive and confidential records. A judgment for monetary damages will not end Defendant's inability to safeguard the PII of Plaintiffs and the Class.

280. Plaintiffs, on behalf of themselves and Class members, seek injunctive relief to enjoin Defendant from further intruding into the privacy and confidentiality of Plaintiffs' and Class members' PII.

281. Plaintiffs, on behalf of themselves and Class members, seek compensatory damages for Defendant's invasion of privacy, which includes the value of the privacy interest invaded by Defendant, the costs of future monitoring of their credit history for identity theft and fraud, plus prejudgment interest, and costs.

COUNT VII
Violation of the California Unfair Competition Law,
Cal. Bus. & Prof. Code §§ 17200 *et seq.*
(On Behalf of Plaintiffs Darbinyan and Lewis and the California Subclass)

282. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

283. Defendant is a "person" defined by Cal. Bus. & Prof. Code § 17201.

284. Defendant violated Cal. Bus. & Prof. Code § 17200 *et seq.* ("UCL") by engaging in unlawful, unfair, and deceptive business acts and practices.

285. Defendant's "unfair" acts and practices include:

a. utilizing cheap, ineffective security measures and diverting those funds to its own profit, instead of providing a reasonable level of security that would have prevented the Data Breach;

b. failing to follow industry standard and the applicable, required, and appropriate protocols, policies, and procedures regarding the encryption of data;

c. failing to timely and adequately notify Class members about the Data Breach's occurrence and scope, so that they could take appropriate steps to mitigate the potential for identity theft and other damages;

d. omitting, suppressing, and concealing the material fact that it did not reasonably or adequately secure Plaintiffs' and Class members' personal information; and

e. omitting, suppressing, and concealing the material fact that it did not comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' personal information, including duties imposed by the FTCA, 15 U.S.C. § 45, and the GLBA.

286. Defendant has engaged in "unlawful" business practices by violating multiple laws,

including the FTCA, 15 U.S.C. § 45, the GLBA, and California common law.

287. Defendant's unlawful, unfair, and deceptive acts and practices include:

a. failing to implement and maintain reasonable security and privacy measures to protect Plaintiffs' and Class members' personal information, which was a direct and proximate cause of the Data Breach;

b. failing to identify foreseeable security and privacy risks, remediate identified security and privacy risks, which was a direct and proximate cause of the Data Breach;

c. failing to comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the GLBA, which was a direct and proximate cause of the Data Breach;

d. misrepresenting that it would protect the privacy and confidentiality of Plaintiffs' and Class members' personal information, including by implementing and maintaining reasonable security measures; and

e. misrepresenting that it would comply with common law and statutory duties pertaining to the security and privacy of Plaintiffs' and Class Members' personal information, including duties imposed by the FTC Act, 15 U.S.C. § 45, and the GLBA.

288. Defendant's representations and omissions were material because they were likely to deceive reasonable consumers about the adequacy of Defendant's data security and ability to protect the confidentiality of consumers' personal information.

289. As a direct and proximate result of Defendant's unfair, unlawful, and fraudulent acts and practices, Plaintiffs and Class members were injured by losing money or property, which would not have occurred but for the unfair and deceptive acts, practices, and omissions alleged herein; spending time and expenses related to monitoring their financial accounts for fraudulent activity; and experiencing an increased, imminent risk of fraud and identity theft, and loss of value of their personal information.

290. Defendant's violations were, and are, willful, deceptive, unfair, and unconscionable.

291. Plaintiffs and Class members have lost money and property as a result of Defendant's conduct in violation of the UCL, as stated herein and above.

292. By deceptively storing, collecting, and disclosing their personal information, Defendant has taken money or property from Plaintiffs and Class members.

293. Defendant acted intentionally, knowingly, and maliciously to violate California's Unfair Competition Law, and recklessly disregarded Plaintiffs' and Class members' rights.

294. Plaintiffs and Class members seek all monetary and nonmonetary relief allowed by law, including restitution of all profits stemming from Defendant's unfair, unlawful, and fraudulent business practices or use of their personal information; declaratory relief; reasonable attorneys' fees and costs under California Code of Civil Procedure § 1021.5; injunctive relief; and other appropriate equitable relief, including public injunctive relief.

COUNT VIII
Violation of the California Consumer Privacy Act
Cal. Civ. Code §§ 1798.100 *et seq.*
(On Behalf of Plaintiffs Darbinyan and Lewis and the California Subclass)

295. Plaintiffs fully incorporate by reference all of the above paragraphs, as though fully set forth herein.

296. The California Consumer Privacy Act ("CCPA"), Cal. Civ. Code § 1798.150(a), creates a private cause of action for violations of the CCPA. Section 1798.150(a) specifically provides:

> Any consumer whose nonencrypted and nonredacted personal information, as defined in subparagraph (A) of paragraph (1) of subdivision (d) of Section 1798.81.5, is subject to an unauthorized access and exfiltration, theft, or disclosure as a result of the business's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information may institute a civil action for any of the following:
>
> (A) To recover damages in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident or actual

damages, whichever is greater.

(B) Injunctive or declaratory relief.

(C) Any other relief the court deems proper.

297. Defendant is a "business" under § 1798.140(b) in that it is a corporation organized for profit or financial benefit of its shareholders or other owners, with gross revenue in excess of $25 million.

298. Plaintiffs and California Class members are covered "consumers" under § 1798.140(g) in that they are natural persons who are California residents.

299. The personal information of Plaintiffs and the Class members at issue in this lawsuit constitutes "personal information" under § 1798.150(a) and 1798.81.5, in that the personal information Defendant collects and which was impacted by the cybersecurity attack includes an individual's first name or first initial and the individual's last name in combination with one or more of the following data elements, with either the name or the data elements not encrypted or redacted: (i) Social Security number; (ii) driver's license number, California identification card number, tax identification number, passport number, military identification number, or other unique identification number issued on a government document commonly used to verify the identity of a specific individual; (iii) account number or credit or debit card number, in combination with any required security code, access code, or password that would permit access to an individual's financial account; (iv) medical information; (v) health insurance information; (vi) unique biometric data generated from measurements or technical analysis of human body characteristics, such as a fingerprint, retina, or iris image, used to authenticate a specific individual.

300. Defendant knew or should have known that its computer systems and data security practices were inadequate to safeguard the Class members' personal information and that the risk

of a data breach or theft was highly likely. Defendant failed to implement and maintain reasonable security procedures and practices appropriate to the nature of the information to protect the personal information of Plaintiff and the Class members. Specifically, Defendant subjected Plaintiffs' and the Class members' nonencrypted and nonredacted personal information to unauthorized access and exfiltration, theft, or disclosure as a result of the Defendant's violation of the duty to implement and maintain reasonable security procedures and practices appropriate to the nature of the information, as described herein.

301. As a direct and proximate result of Defendant's violation of its duty, the unauthorized access and exfiltration, theft, or disclosure of Plaintiffs' and Class members' personal information included exfiltration, theft, or disclosure through Defendant's servers, systems, and website, and/or the dark web, where hackers further disclosed the personal identifying information alleged herein.

302. As a direct and proximate result of Defendant's acts, Plaintiffs and the Class members were injured and lost money or property, including but not limited to the loss of Plaintiffs' and Class members' legally protected interest in the confidentiality and privacy of their personal information, stress, fear, and anxiety, nominal damages, and additional losses described above.

303. Section 1798.150(b) specifically provides that "[n]o [prefiling] notice shall be required prior to an individual consumer initiating an action solely for actual pecuniary damages."

304. On March 26, 2025 and March 27, 2025, pursuant to California Civil Code § 1798.150(b), Plaintiffs mailed CCPA notice letters to Defendant's registered service agents, detailing the specific provisions of the CCPA that Defendant has violated and continues to violate. Defendant has not cured the violations within 30 days—and Plaintiffs believe such cure is not

possible under these facts and circumstances—thus Plaintiffs seek statutory damages as permitted by the CCPA in an amount not less than one hundred dollars ($100) and not greater than seven hundred and fifty ($750) per consumer per incident, or actual damages, whichever is greater pursuant to Cal. Civ. Code § 1798.150(a)(1)(A) & (b) as well as actual pecuniary damages suffered as a result of Defendant's violations described herein.

VII. REQUEST FOR RELIEF

WHEREFORE, Plaintiffs on behalf of themselves and other members of the Class proposed in this Complaint, respectfully request that the Court enter judgment in their favor and against Defendant, as follows:

A. Declaring that this action is a proper class action, certifying the Nationwide Class as requested herein, designating Plaintiffs as Nationwide Class Representatives, and appointing Class Counsel as requested in Plaintiffs' anticipated motion for class certification;

B. Ordering Defendant to pay statutory damages to Plaintiffs and California Subclass members;

C. Ordering Defendant to pay actual damages to Plaintiffs and the other members of the Class;

D. Ordering Defendant to pay punitive damages, as allowable by law, to Plaintiffs and the other members of the Class;

E. Ordering injunctive relief requiring Defendant to, *e.g.*: (i) strengthen their data security systems and monitoring procedures; (ii) submit to future annual audits of those systems and monitoring procedures; and (iii) immediately provide free credit monitoring to all Class members;

F. Ordering Defendant to pay attorneys' fees and litigation costs to Plaintiffs and Plaintiffs' counsel;

G. Ordering Defendant to pay equitable relief, in the form of disgorgement and restitution, and injunctive relief as may be appropriate;

H. Ordering Defendant to pay both pre- and post-judgment interest on any amounts awarded; and

I. Ordering such other and further relief as may be just and proper.

VIII. JURY TRIAL DEMANDED

Plaintiffs hereby demand that this matter be tried before a jury.

Dated: June 16, 2025

Respectfully Submitted,

/s/ Mariya Weekes
Mariya Weekes (*admitted pro hac vice*)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
201 Sevilla Avenue, 2nd Floor
Coral Gables, FL 33134
Tel: (786) 879-8200 / Fax: (786) 879-7520
mweekes@milberg.com

/s/ Thomas A. Pacheco (signed w/permission)
Thomas A. Pacheco (Bar No. 21639)
MILBERG COLEMAN BRYSON PHILLIPS GROSSMAN, PLLC
900 W Morgan Street
Raleigh, NC 27603
T: (212) 946-9305
tpacheco@milberg.com

Andrea R. Gold (D. Md. Bar No. 18656)
TYCKO & ZAVAREEI LLP
2000 Pennsylvania Ave. NW, Suite 1010
Washington, D.C. 20006
Phone: (202) 973-0900
Email: agold@tzlegal.com

Manuel S. Hiraldo (*pro hac vice* forthcoming)
HIRALDO P.A.
401 E Las Olas Blvd., Suite 1400
Ft. Lauderdale, FL 33301
Phone: (954) 400-4713
Email: mhiraldo@hiraldolaw.com

Jason S. Rathod (Bar. No. 18424)
Nicholas A. Migliaccio (Bar No. 29077)
Migliaccio & Rathod LLP
412 H Street NE
Washington, DC 20002
Phone: (202) 470-3520
Fax: (202) 800-2730
Email: jrathod@classlawdc.com
nmigliaccio@classlawdc.com

Andrew Shamis (admitted *pro hac vice*)
SHAMIS & GENTILE, P.A.
14 NE 1st Ave, Suite 705
Miami, FL 33132
Phone: (305) 479-2299
Email: ashamis@shamisgentile.com

Jeff Ostrow (*pro hac vice* forthcoming)
KOPELOWITZ OSTROW P.A.
One West Las Olas Blvd., Suite 500
Fort Lauderdale, FL 33301
Phone: (954) 525-4100
Email: ostrow@kolawyers.com

Duane O. King (Bar No. 19430)
The Law Offices of Duane O. King
803 W. Broad St. Suite 210
Falls Church, VA 22046
Phone: (202) 331-1963
Fax: (202)449-8365
Email: dking@dkinglaw.com

Leigh S. Montgomery (*pro hac vice* forthcoming)
EKSM, LLP
4200 Montrose Blvd., Suite 200
Houston, Texas 77006
Phone: (888) 350-3931
Email: lmontgomery@eksm.com

Mona Amini (*pro hac vice forthcoming*)
KAZEROUNI LAW GROUP, APC
California Bar No. 296829
245 Fischer Avenue, Unit D1
Costa Mesa, California 92626
Telephone: (800) 400-6808
Facsimile: (800) 520-5523
Email: mona@kazlg.com

Counsel for Plaintiffs and Putative Class

CERTIFICATE OF SERVICE

I hereby certify that on this date, June 16, 2025, I filed the foregoing ***Consolidated Class Action Complaint*** with the Clerk of the Court via the Court's electronic filing system, which will provide electronic mail notice to all counsel of record.

/s/ Mariya Weekes
Mariya Weekes (*admitted pro hac vice*)